M1MI2016 Codes et Cryptologie

Feuille d'exercices n° 1.

Arithmétique

1 Si $a = 462$ et $b = 104$, calculez $d = \text{pgcd}(a, b)$, ainsi que deux entiers u et v tels que $au + bv = d$. Calculez $\text{ppcm}(a, b)$.

2 Calculez par la méthode de votre choix les pgcd suivants : $\text{pgcd}(46848, 2379)$, $\text{pgcd}(13860, 4488)$, $\text{pgcd}(42098, 36146)$, $\text{pgcd}(30076, 12669, 21733)$, $ppgcd(4096, 11111111111111)$.

3 Montrez que $\text{pgcd}(ab, ac) = a\,\text{pgcd}(b, c)$.

4 Montrez que $\text{pgcd}(2n^3 + 5n^2 + 4n + 1, 2n^2 + n) = 2n + 1$.

5 **Le Lemme de Gauss.** Montrez que, si $a|bc$ et $\text{pgcd}(a, b) = 1$, alors $a|c$.

6 Trouvez deux entiers u et v tels que $29u + 24v = 3$, puis déterminez tous les couples $(u, v) \in \mathbb{Z}^2$ tels que $29u + 24v = 3$. Mêmes questions pour $30u + 35v = 100$, $13u + 19v = 4$.

7 Soit $d = \text{pgcd}(a, b)$. Déterminez tous les couples $(u, v) \in \mathbb{Z}^2$ tels que $d = au + bv$.

8 Démontrez les résultats suivants :

1. Si a divise c et b divise c et si $\text{pgcd}(a, b) = 1$ alors ab divise c.
2. Si $\text{pgcd}(a, b) = 1$ et si $\text{pgcd}(a, c) = 1$ alors $\text{pgcd}(a, bc) = 1$.
3. Si p est un nombre premier et si p divise ab alors p divise a ou p divise b.

9 Faire la liste des nombres premiers inférieurs à 100. On pourra utiliser le crible d'Ératosthène.

10 **Nombres de Mersenne.** Un nombre de Mersenne est un nombre entier de la forme $M_p = 2^p - 1$. Montrez que, si M_p est premier, alors p est premier (on pourra utiliser la formule $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$). Vérifiez que M_2, M_3, M_5, M_7 sont premiers mais pas M_{11}. *On connait 47 nombres premiers de Mersenne. On conjecture qu'il en existe une infinité.*

11 **Nombres parfaits.** Un entier positif a est un nombre parfait si la somme de ses diviseurs positifs est égale à $2a$. Montrez que, si $a = 2^n p$ avec p premier, a est parfait si et seulement si $p = 2^{n+1} - 1$. En déduire que p est un nombre premier de Mersenne et donc que $n + 1$ est un nombre premier (voir l'exercice sur les nombres de Mersenne). Calculez les quatre premiers nombres parfaits.

12 **Nombres de Fermat.** Un nombre de Fermat est un nombre entier de la forme $F_n = 2^{2^n}+1$.

1. Montrez que, si $2^a + 1$ est premier, alors a est nécessairement une puissance de 2 (on pourra utiliser la formule : si n est impair, $x^n + 1 = (x + 1)(x^{n-1} - x^{n-2} + \cdots - x + 1)$).
2. Vérifiez que F_0, F_1, F_2, F_3, F_4 sont premiers, mais que F_5 n'est pas premier (on pourra chercher un facteur de la forme $128k + 1$).
3. Montrez les propriétés suivantes :

$$F_n = (F_{n-1} - 1)^2 + 1$$
$$F_n = F_{n-1} + 2^{2^{n-1}} F_0 \dots F_{n-2}$$
$$F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$$
$$F_n = (F_0 F_1 \dots F_{n-1}) + 2$$

   et déduire de la dernière qu'il sont deux à deux premiers entre eux.

On ne connait aucun autre nombre premier de Fermat..

13 **Plimpton 322**

`http://www.columbia.edu/cu/lweb/eresources/exhibitions/treasures/html/158.html`
On appelle *triplet pythagoricien* un triplet d'entiers (a, b, c) tels que $a^2 + b^2 = c^2$. Le but de cet exercice est de décrire tous les triplets pythagoriciens.

1. Montrez que, si m et n sont des entiers premiers entre eux, alors

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2 \tag{1}$$

   est un triplet pythagoricien.

Dans la suite, on suppose que a, b, c n'ont aucun diviseur commun, et que $a^2 + b^2 = c^2$. Notre but est de montrer qu'alors (a, b, c) est de la forme (1).

2. Montrez que $\text{pgcd}(a, b) = \text{pgcd}(b, c) = \text{pgcd}(c, a) = 1$.
3. Montrez que a ou b est pair.

On suppose désormais que b est pair et on pose $b = 2b'$.

4. Montrez que $u = (c + a)/2$ et $v = (c - a)/2$ sont entiers et premiers entre eux.
5. Montrez que $uv = b'^2$ et en déduire que u et v sont des carrés d'entiers.
6. Conclure.
7. Pour quelles valeurs de m et n obtient-on $a = 10441$ et $c = 20809$?

14 Euclide a décidé de travailler sur les entiers écrits en base 2 pour se préparer à la révolution numérique.

Si $a = a_0 + 2a_1 + 4a_2 + \cdots + 2^n a_n$ avec $a_k = 0, 1$ est l'écriture binaire de a, il note $a = a_n a_{n-1} \ldots a_1 a_0$.

1. Écrire en binaire les nombres 16, 13, 280.
2. Convertir en base 10 le nombre binaire 101010.
3. Quel est l'effet de la multiplication par une puissance de 2 sur un nombre binaire ?
4. Posez et effectuez l'addition et la soustraction de $a = 11100010$ et $b = 10011111$.

Euclide souhaite effectuer son célèbre algorithme sur des nombres binaires, mais comme il a du mal avec les multiplications et les divisions, il remplace les divisions euclidiennes $a = bq + r$ par $a = b2^k + r$ où il prend k le plus grand possible tel que $b2^k \leq a$.

5. Expliquez pourquoi, dans l'exécution de son algorithme, Euclide va parfois obtenir un reste plus grand que le diviseur. Que doit-il faire dans ce cas ? Exemple : $a = 1101$ et $b = 100$.
6. Effectuez cet algorithme sur $a = 100001010$ et $b = 111000$ pour calculer leur pgcd.
7. Montrez que, dans cette pseudo-division euclidienne, $r < a/2$.
8. En déduire que, dans la suite des restes successifs $r_0 = a$, $r_1 = b, \ldots, r_k, \ldots$ calculés au cours de l'algorithme, on a $r_k < a/2^{k/2}$.
9. En déduire que le nombre de pseudo-divisions dans cet algorithme est au plus deux fois le nombre de chiffres binaires de a.
10. À l'aide de ce qui précède, comparer le nombre de divisions euclidiennes effectuées pour calculer le pgcd de deux entiers, d'une part dans l'algorithme d'Euclide, et d'autre part dans la méthode consistant à d'abord factoriser ces entiers par divisions successives.